RAPID7

SERVICE BRIEF

PREEMPTIVE MDR FOR YOUR MICROSOFT ENVIRONMENT

MDR FOR MICROSOFT

Expert managed threat detection, investigation, and response to maximize and protect your Microsoft investment

As the backbone of productivity and security for many organizations, Microsoft ecosystems collectively represent one of the largest attack surfaces in the world. Many organizations adopt comprehensive E5 licenses for the value of Office productivity, Defender security, or both. But the same breadth of tooling that enables efficiency often compounds the challenges already overwhelming security operations teams: high alert volumes that obscure real risk, insufficient staff and expertise to manage complex technology, and limited ability to drive a truly proactive, resilient security posture.

Enter Rapid7 MDR for Microsoft

Rapid7 is a trusted provider of Managed Detection and Response for thousands of organizations worldwide, delivering a 422% three-year ROI and reducing the chance of a major security event by 54% in any given year.[1] Our service combines preemptive SOC triage and investigation to detect and respond to threats, dedicated technical guidance to help teams continuously mature their defenses, and transparent service delivery that links security outcomes to business value.

With MDR for Microsoft, these capabilities are now extended deeper into your Microsoft environment – operationalizing Microsoft Defender to reduce noise and surfacing the threats that matter. The result: stronger threat coverage, less analyst fatigue, and greater resilience across the attack surface.

Make the most of your existing footprint

Preempt attacks before they start

By correlating Microsoft Defender telemetry with real-world vulnerability risk and Rapid7’s broader environmental context, we surface the attack paths that matter most, cutting dwell time, shrinking blast radius, and stopping attacks before impact.

Respond with certainty across the full attack lifecycle

AI-assisted, expert-led investigations drive rapid containment and active remediation, including remote response with Velociraptor and unlimited incident response. From alert through recovery, our SOC ensures threats are eradicated and operations stay online.

Strengthen resilience through partnership

Your dedicated Cybersecurity Advisor and the Rapid7 SOC turn incidents into insight, delivering actionable recommendations, refined detections, and ongoing hardening that strengthens defenses and builds lasting cyber resilience.

Get better outcomes from Microsoft – not overhead

Transform your Microsoft Defender infrastructure into the foundation for more effective security – prioritizing real risk, driving decisive action, and delivering measurable outcomes without added tools, teams, or operational burden.

Enhanced protection across key vectors

DEFENDER FOR ENDPOINT

Endpoints face constant pressure from ransomware, malware, credential theft, and hands-on-keyboard attacks.

Rapid7 unifies Defender endpoint alerts with cross-vector context to deliver high-fidelity investigations, faster triage, and more accurate threat validation. With Active Response and Velociraptor DFIR, we remotely contain threats and perform deep forensic analysis, supported by bidirectional integration that keeps both Rapid7 and Defender consoles aligned.

DEFENDER FOR IDENTITY

Identity compromise is now the most common breach vector, with attackers exploiting password spray, token theft, lateral movement, and privilege escalation to avoid endpoint-only detection.

Alongside UEBA baselines, authentication patterns, and risk insights, Defender for Identity signals help reconstruct user behavior, validate true compromise, and map lateral movement paths. This context is woven into investigations, enabling faster, higher-confidence conclusions and shaping response actions.

DEFENDER FOR CLOUD

Azure environments evolve rapidly, creating misconfigurations, stale resources, excessive permissions, and cloud-native attack paths that are easy for adversaries to exploit and hard for teams to track.

Rapid7 correlates cloud alerts with asset context to understand the significance of suspicious API calls, resource manipulation, privilege escalation, or anomalous service behavior – ensuring threats affecting Azure resources are fully understood within the broader attack campaign.

DEFENDER FOR OFFICE 365

Email is a prime entry point for phishing, business email compromise, credential harvesting, and mailbox manipulation.

Rapid7 analysts leverage Office 365 signals to validate whether email-based alerts indicate user error, benign automation, or true adversary activity. The SOC uncovers impersonation attempts, persistence mechanisms, and lateral movement hidden within messaging workflows – adding crucial investigative context that shapes the direction and urgency of investigations.

Key capabilities and services

HUMAN & AI-POWERED PROTECTION

- **24×7×365 SOC monitoring** for continuous, expert-led detection and investigation across your Microsoft environment, ensuring threats are identified and acted on at all times.
- **Unlimited Incident Response & Embedded DFIR** delivers end-to-end breach response without additional retainers or time caps, enabling Rapid7 experts to investigate, contain, and fully neutralize threats until your environment is secure.
- **Dedicated Cybersecurity Advisor** for monthly security posture reviews, threat briefings, alert tuning, and strategic program guidance to help build security resilience.
- **Active Response & Remediation** executes rapid, policy-driven containment and remediation actions – such as host isolation, account disablement, or deletion of malicious files – preventing lateral movement and eradicating threats before they escalate.
- **Proactive Threat Hunting identifies** emerging threats and suspicious behavior across your ecosystem before they trigger alerts, reducing attacker dwell time and improving resilience.

MICROSOFT INTEGRATION & EVENT SOURCE COVERAGE

- **E5 Security License Coverage** leverages your existing Defender licensing to operationalize telemetry across Endpoint, Identity, Cloud, and Email – maximizing operationalization and ROI of your Microsoft investment.
- **Bi-Directional Defender Integration** synchronizes endpoint alert status and analyst actions between Rapid7 and Microsoft consoles, eliminating noise, keeping systems aligned, and reducing the need to context switch to reconcile alerts.

RAPID7 PRODUCT CAPABILITIES

- **Enterprise Vulnerability Risk Management** identifies, prioritizes, and contextualizes exposures across your Microsoft and hybrid environments, enabling focus on the vulnerabilities most likely to be exploited by threats.
- **Unlimited SOAR** automates investigation steps, response actions, and cross-tool workflows to accelerate containment and reduce analyst burden – saving time and stopping attackers in their tracks.
- **Unlimited Data Ingestion** eliminates ingestion-based SIEM cost constraints and ensures complete visibility across Microsoft, Rapid7, and third-party sources so no critical signals are missed.
- **AI-Enhanced SOC** for accelerated triage of benign alerts with 99.93% accuracy, autonomous gathering of contextual data that empowers human decision-making, and natural language log querying for surfacing insights without complexity.
- **13 Months Data Retention** provides long-term visibility, enabling your team and our analysts to correlate activity over extended timelines and uncover stealthy adversary behavior that shorter retention windows miss.
- **Hosted Velociraptor** delivers deep forensic visibility and rapid endpoint interrogation to support high-fidelity investigations, root-cause analysis, and evidence-driven incident response.

Get **422% ROI** and **reduce the chance of a major security event by more than half** with Rapid7 MDR

IDC BUSINESS VALUE STUDY

1 The Business Value of Rapid7 Managed Detection and Response, IDC

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**